



INFORMATION TECHNOLOGY POLICY

JULY 2021

1155 28TH STREET SW
WYOMING, MI 49509
PHONE: (616) 530-3173
FAX: (616) 261-7103
www.wyomingmi.gov

INFORMATION TECHNOLOGY DEPARTMENT
HELP DESK – (616)-261-3524
FAX: (616)-530-3177
E-MAIL: helpdesk@wyomingmi.gov

TABLE OF CONTENTS

<u>SECTION</u>	<u>CONTENTS</u>	<u>PAGE</u>
	<u>Community Commitment</u>	1
	<u>Policy</u>	1
1	Policy Approval.	1
	A. City Manager Approval.	1
	B. Modification	1
	C. Notice of Modification	1
2	Required Compliance.	1
	A. Applicability and Requirement.	1
	B. Acknowledgement Required.	1
3	Definitions and Interpretation.	1
	A. Definitions.	1
	B. City Officers	3
	C. Agencies.	3
4	Use Conditions and Authorization.	3
	A. Use Conditions.	3
	B. Authorization Process.	3
	C. Authorization Is Limited.	4
	D. Authorization Changes or Termination.	4
5	Privacy.	4
	A. City's Reserved Rights.	4
	B. User Rights Limited.	4
	C. IT Staff Duties.	5
	D. City Supervisory Rights.	5
	E. Records Disclosure.	5
	F. Personal Device Disclosure.	5
	G. Consent.	5
6	Confidentiality.	5
	A. All City Content Is Confidential.	5
	B. Additional Legal Requirements.	5
7	Security.	6
	A. Security Risk.	6
	B. Security Responsibility.	6
	C. Passwords.	6
	D. Multi-factor Authentication.	7
	E. Security Training.	7
	F. Responsibility to Recognize and Report.	7
	G. Account Lockout Due to Password Expiration or Other Reason.	7
8	Appropriate Use.	8
	A. General Expectations and Requirements.	8
	B. Software and Applications.	8
	C. Copyrighted Material – Intellectual Property Rights.	8
	D. Use of City Email.	8
	E. Personal Email Access and Use.	9
	F. Personal Use of City Devices and Computing Environment.	9
	G. Internet Use.	9
	H. Storage of Files & Encryption.	10
	I. Cloud Computing.	10
	J. Prohibited Use.	11
	K. Use Cautions.	12
9	Personal Devices.	12
	A. City Rights.	12
	B. Permission Required.	12

<u>SECTION</u>	<u>CONTENTS</u>	<u>PAGE</u>
10	Physical Security.	13
	A. Auto-lock.	13
	B. User Lock and Lockout.	13
	C. Securing Devices and Information.	13
	D. Prohibited Device Connections.	13
	E. Device Loss, Theft or Tampering.	13
	F. Equipment Relocation.	13
11	Remote Access.	13
	A. Allowed Use.	13
	B. Authorized Users and Devices.	13
	C. Approved Access Methods.	14
	D. VPN Approval.	14
12	Electronic Device and Software Acquisition.	14
13	Disposal of City Devices.	14
	A. General Disposal by IT Department.	14
	B. Cell Phones.	14
14	Information, Data and Content Disposal.	14
15	City Messaging.	14
	A. Prohibited Messaging.	14
	B. Prohibited Use of Personal Device.	15
16	Social Media.	15
	City Manager's Certification and Signature.	15
	Employee Receipt of Information Technology Policy.	16
	Non-Employee User Receipt and Acknowledgement of Information Technology Policy.	17

COMMUNITY COMMITMENT

The City of Wyoming envisions a “diverse, strong, and authentic community where all individuals have the opportunity to thrive.” Wyoming’s seeks to accomplish that mission by focusing on “community, safety and stewardship.” Thus, the city is committed to ensuring all community members and all personnel (i) feel included, vital, important, understood, and valued, (ii) are treated respectfully, courteously, compassionately, and with dignity, and (iii) feel safe and are free from intimidation or oppression. Wyoming is also committed to prudently and responsibly using community resources.

Several truths about information technology underlie this policy. Information technology, both devices and uses of them, are tools that, when used properly (as intended), responsibly (in a manner to avoid adverse consequences), and effectively (to maximize its possible benefits), can enhance city services to the community and enhance the working environment for city personnel. Using information technology in other ways can jeopardize relationships, disclose confidential information enabling its misuse, impair security of persons and infrastructure, incur legal risks, disrupt city and other operations, tie-up significant personnel and financial resources, and wreak systemic havoc. In some cases, information technology misuse contributed to injury and death. Attempts by persons outside city government to access, manipulate, vandalize, corrupt, destroy, steal, appropriate for improper use, disable, or otherwise adversely affect the city computing environment, city devices, city information and data, city owned or used software, and personal devices are ongoing, increasingly sophisticated, and increasingly difficult to prevent.

Therefore, Wyoming is committed to best practices for using information technology. Accordingly, the principles underlying and requirements and limitations within this policy are intended to reflect best practices. City leaders view this policy and compliance with it as key parts of the relationships among city personnel and between city personnel and the community. They are also key to local government excellence.

INFORMATION TECHNOLOGY POLICY

§1 – Policy Approval.

- A. City Manager Approval. The city manager’s approval and signature makes this official city policy.
- B. Modification. The city may add to or modify this policy at any time.
- C. Notice of Modification. When the policy is changed, notices will be provided to users and, if required under a collective bargaining agreement, to union representatives in writing or by email using the city’s email system. Notice of policy changes must be approved by the IT director.

§2 – Required Compliance.

- A. Applicability and Requirement. All city personnel and all city bodies must comply with this policy. Noncompliance can have the same consequences as noncompliance with any other city policy. (See §4.A.2.)
- B. Acknowledgement Required. All city personnel and all users must sign the acknowledgement of this policy and return it to their supervisors or the city HR director. Users who are city contractors must return the signed acknowledgement to the city IT director.

§3 – Definitions and Interpretation.

- A. Definitions. The following definitions apply to words and phrases in this policy unless the context clearly indicates otherwise:
 - 1. *City* or *Wyoming* means the City of Wyoming, Kent County, Michigan.
 - 2. *City bodies* or *Wyoming bodies* means the City Council and all boards, bodies and commissions of, created by, or under the purview of Wyoming including, for example, the Downtown Development Authority, Brownfield Redevelopment Authority, Historical Commission, Housing Commission, Community Enrichment Commission, Community Development Committee, and Economic Development Corporation. The 62-A District Court is a city body for purposes of this policy, though it is partially a state agency which may affect some consequences for some policy violations under some circumstances. (Nonprofit entities contracting with the city to use city facilities or to provide

programs or services at city facilities, such as the Greater Wyoming Community Resource Alliance, Wyoming Senior Fellowship, and Pinery Park Little League, are city contractors as defined below and must comply with this policy under subsection 7.B.)

3. *City contractors* means any individual or entity, other than city personnel or a city body, that has entered a contract with Wyoming or a city body to provide any goods, services, or programs to or for Wyoming or any city body, including, without limitation (i) the design, construction, installation, maintenance, repair or improvement, or replacement of any city property, (ii) professional services or consultation, (iii) training of any kind, (iv) programs related to parks, the Wyoming Senior Center, TEAM 21 or other after-school program, or other community activities, (v) maintenance or repair of any city vehicles or other personal property, (vi) mowing or snowplowing of city property or rights-of-way, (vii) refuse or waste collection or disposal, (viii) computer or other hardware or software design, supply, or services, (ix) cleaning or janitorial services, (x) CDBG or other HUD program services, and (xi) office, shop, laboratory, or other supplies and equipment.

4. *City Council* means the Wyoming City Council.

5. *City device(s)* means one or more electronic devices (networked or stand-alone) owned by, leased by, or supplied by the city to any city personnel.

6. *City manager* means the duly appointed or acting city manager of the city.

7. *City personnel* or *Wyoming personnel* means all elected and appointed officers, employees, volunteers, and other agents of the City of Wyoming. This includes personnel of the Wyoming Housing Commission and, except as otherwise limited by applicable law, 62-A District Court personnel.

8. *Civil Rights Policy* means the Civil Rights Policy approved by the City Council as supplemented or amplified by explanatory, directive, training, or other materials provided by the city manager or the HR department.

9. *Computing environment* means city devices and uses that can be made of them, physical and logical networks, servers, storage, software, use rights, applications or capabilities (including but not limited to any that are hosted or controlled by third parties under contractual agreements with the city, e.g., Cloud-based applications or storage). It includes the city's telephone system and connected equipment. Computing environment does not include personal devices though their use in connecting to the computing environment may affect the computing environment.

10. *Department head* means a duly appointed individual serving in a department head role as designated by the city manager or city council or that individual's designee.

11. *Electronic device* means any device that can be used to receive, transmit, store, retrieve, process, manipulate, record, display, play, amplify, configure, or reconfigure any sound, image, words, symbols or other information or data that in electronic format(s) of any kind also including, for example and without limitation, any device that changes the format of any sound, image, words, symbols or other information or data from non-electronic to electronic or from electronic to non-electronic formats. This includes, for example and not for limitation, desktop computers, laptop computers, tablet computers, notebook computers, netbooks, smart phones, cellular phones, other data-enabled cellular devices, flash or thumb drives, other data storage devices, external drives, CD or video players, copiers, tape recorders or players, video recorders, radios, televisions, broadcasting equipment, servers, body-worn cameras and sound recorders, vehicle-based cameras and sound recorders, meters and other measuring devices, electronic diagnostic and testing devices, evidence storage and retrieval equipment, and any similar device(s).

12. *HR director* means the city's director of human resources.

13. *Information technology* means electronic devices, software, operating systems, cloud-based services and storage, broadband, internet, internet access, and any use of and all means of accessing or using electronic devices or electronic information or data.

14. *IT department* means the city's Information Technology Department.

15. *IT director* means the director of the IT Department.

16. LAN means the local area network that is a part of the computing environment.

17. *Person* means an individual, corporation, professional corporation, limited liability company, partnership, association, trust, governmental entity or agency, or other recognized entity or group.

18. *Personal device(s)* means one or more electronic devices other than a city device that is owned by, leased by, or used by a person.

19. *User* means any person using any electronic device and/or accessing or using the computing environment.

B. City Officers. Identification of a city official by title includes that official's superiors and designee(s).

C. Agencies. Identification of any federal or state agency by name or any city department by name includes its successor agency or department.

§4 – Use Conditions and Authorization.

A. Use Conditional. Access to and use of any city device or the computing environment is conditional upon acknowledgement of and compliance with this policy.

1. A failure to comply with this policy may result in immediate suspension and/or termination of access to or use of city devices and/or computing environment. Lack of access to city devices and/or the computing environment may result in an inability to perform employment duties and then result in termination of employment.

2. Just as for any other city policy, a failure to comply with this policy can result in other consequences. Because many violations of this policy significantly and adversely affect other users, city personnel, the city, and other persons, other consequences for violations can be significant.

- a. Violations of this policy may have significant employment consequences for city employees up to and including employment termination.
- b. Violations of this policy constitute misfeasance and malfeasance in office.
- c. Violations of this policy may be crimes.
- d. Violations of this policy may result in personal liability.

B. Authorization Process.

1. Authorization for new city employees shall be undertaken as follows:

- a. HR department staff should ask new employees to confirm and, if possible during background or reference checks, ascertain whether the new employee has had any information technology use rights suspended, terminated, or threatened with suspension or termination due to a failure to comply with user conditions, policies or requirements. If a new employee has had a situation in which that occurred, HR department staff should inquire further about the circumstances, including when it occurred, what happened, and what resulted from the situation. That additional information should be reviewed with the director of the hiring city department and, if desirable, the IT director, city attorney, and/or city manager to determine whether it affects the hiring decision or the user authorizations to be provided the new employee.
- b. The department to whom the new employee will be assigned must notify the IT helpdesk at least 7 days before the new employee's start date with the following information:
 - i. The new employee's name, title or position, work location, supervisor(s)' name(s), and general information about assigned duties.
 - ii. A list of any city devices to be provided the new employee.
 - iii. A description of the new employee's required access and limitations of access to the computing environment.

2. Applications and background checks for city volunteers, including members of city boards and commissions, who will be users must include questions about whether the individual has had any information technology use rights suspended, terminated, or threatened with suspension or termination due to a failure to comply with user conditions, policies or requirements. If the individual has had a situation in which that occurred, city staff should inquire further about the circumstances,

including when it occurred, what happened, and what resulted from the situation. That additional information should be reviewed with the director of the city department engaging the volunteer or the appointing person(s) for the board or commission member, and, if desirable, the IT director, city attorney, and/or city manager to determine whether it affects the engagement or appointment of the applicant or the user authorizations to be provided the volunteer/appointee.

3. Authorization to access the computing environment with personal devices requires the approval of (i) the director of the department to whom the city personnel is assigned or with which a city contractor is working, (ii) the IT director, and (iii) the city manager. See additional information in §9.

4. Authorization for city contractors will follow the same course as for city employees, though access to city devices and the computing environment will be more strictly limited and will require approval from the affected department head, the IT director, and city manager.

C. Authorization Is Limited.

1. Authorization for access to or use of city devices or the computing environment will generally be limited to city devices and parts of the city computing environment reasonably needed or helpful to performing job functions. If city personnel or contractors need only intermittent or temporary access to some data, programs, or devices, that access may be authorized and enabled only when it is needed.

2. Access to or use of some data, data bases, software, programs, or devices (e.g., federal tax information data, medical information, law enforcement data bases, etc.) is limited by law and will be authorized only as provided by applicable law.

3. Access to or use of data, data bases, software, programs, and city devices may require additional authorization by department directors in addition to that to which city personnel is assigned or city contractors are working, the IT director, city manager, or others. Consult the IT director regarding such data, data bases, and devices.

4. Any use of or access to a city device or the computer environment by any person (i) in a manner that is not authorized, (ii) for any unauthorized purpose, (iii) at any unauthorized time or in an unauthorized place, (iv) from an unauthorized electronic device, (v) for an unauthorized use, (vi) contrary to any legal requirements, prohibitions, or limitations, (vii) in violation of this policy, is prohibited.

D. Authorization Changes or Termination.

1. Changes in authorization - to broaden it, narrow it, terminate it, add additional electronic devices, or otherwise alter it – should be initiated by the supervisory city personnel for city personnel and contractors by a written request to the IT helpdesk at least 7 days before the change is desired to occur. The request should include as much of the information as is provided in subsection 4.A.1.b.

2. If the employment or engagement of any user is ending for any reason (e.g., retirement, resignation, termination, expiration of a term of office, removal from office, contract expiration, contract nonrenewal, contract termination, etc.) or the user is suspended, or placed on paid or unpaid leave, the department head for the city department to which the city employee was assigned, which liaison's with the other city personnel (e.g., board or commission members or volunteers), or that is working with a contractor, must:

a. Notify the IT director so that user's access to and use of city devices or the computing environment can be terminated or otherwise appropriately controlled.

b. Retrieve from the city personnel or contractor any city devices and return them to the IT department.

c. Notify the IT director about who should be provided access to the departing city personnel or contractor's e-mail, files, directories, etc. to ensure communications and data are appropriately handled and maintained in accordance with city policies, including records retention requirements.

§5 – Privacy.

A. City's Reserved Rights. To the maximum extent allowed by law, **the city reserves and may exercise its right to monitor, intercept, archive, view, or distribute any communications and/or content**

transmitted over or using any city device or the computing environment.

B. User Rights Limited. **No user will have any expectation of privacy in the access or use of any city device or the computing environment.**

C. IT Staff Duties. IT department staff charged with operating and maintaining the computing environment, including city devices, may, from time to time, need to or be directed to access all material and content currently or previously in the computing environment. IT department staff may load agents or software applications on city devices to aid in administration of the city devices, such as auto-populating cell phones with city resources, requiring certain levels of security, and locating or wiping lost devices.

D. City Supervision. Department directors, the city manager, or HR department staff, may monitor city personnel's use of the Internet and email and may revoke authorization to use or access any part of the computing environment, including email and the Internet by notifying the IT director or HR director.

E. Records Disclosure. Any records on any city device or the computing environment may be subject to records requests either under Michigan's Freedom of Information Act, or pursuant to judicial or administrative process. This includes all email messages, text messages, voice messages, facsimile transmissions, photos, and any file, image, sound or other sharing.

F. Personal Device Disclosure. If personal devices are used by city personnel for any communications or other uses related to city matters, they too may be subject to those records requests and, in some cases, could be physically turned over to and viewed by forensic experts engaged by outside parties.

G. Consent. **A user's access to or use of a city device or the computing environment constitutes the user's consent to city monitoring and any review of the user's access and/or use of the city device or the computing environment.**

§6 – Confidentiality.

A. All City Content Is Confidential. **All information, data and content on city devices or the computing environment is confidential.** Only authorized persons, may access, use, or and release it and only in accordance with city policies. **Access, use, or release of any information, data and content on city devices or the computing environment by any persons other than those authorized to do or in any manner except as authorized in accordance with city policies is prohibited.**

B. Additional Legal Requirements. By law, some information is especially sensitive requiring the utmost degree of care to prevent disclosure and the disclosure of some information, even inadvertently, can have significant legal consequences.

1. Illustrative examples of sensitive, confidential information include:
 - a. Any records with Social Security numbers, driver's license numbers, or other special identification numbers.
 - b. Information with an individual's date of birth.
 - c. Addresses, email addresses, cell phone numbers, land line numbers, and similar information for individuals listed on certain lists maintained by the state.
 - d. Information with credit card, banking, and other financial numbers and information.
 - e. Information from the Law Enforcement Information Network (LEIN), National Criminal Information Center (NCIC), Michigan Department of State, or similar traffic or law enforcement data bases.
 - f. Medical records or receipts, mental health records or receipts, pharmacy records or receipts, and other health records.
 - g. Security information about city facilities, businesses, or residents.
 - h. Juvenile arrest and court records.
 - i. Educational records related to students.
 - j. Many personnel records.
 - k. Records that might disclose proprietary processes, technology, or other business records.
 - l. Records that might disclose the nature, quantities, locations or other information about certain substances and materials.
 - m. Records related to possible economic development projects or property transactions.

- n. Records classified under law as “federal tax information.”
 - o. Records used to establish income or other eligibility for federal, state, county or city support or programs.
 - p. Personal information gathered for statistical or other purposes such as any individual’s race, ethnicity, gender identity, sexual orientation, national origin, height, weight, faith, marital status, familial status, criminal record, driving record, genetic information, fingerprints or other biometric information, facial or other images, sources of income, finances, etc.
 - q. Information that may be subject to attorney-client, attorney work product, accountant-client, clergy-penitent, counselor-patient, physician-patient, or other privileges.
 - r. Crime victim and witness information.
 - s. Parts of election records.
 - t. Some images or sound recordings captured on body-worn or vehicle cameras or devices.
 - u. Bids and bidder information prior to public opening of them.
 - v. Information related to the locations of some archaeological sites or artifacts.
 - w. Some test results related to students, personnel matters, etc.
 - x. Other information that is protected by applicable law, court or administrative agency order, contract, or other legal obligation, requirement, or restriction.
2. Management of such information requires extra care and awareness to prevent a breach of security and confidentiality. Accordingly, users must:
- a. Not leave confidential documents on a remote/shared printer in an unsecured area where documents may be read by others.
 - b. Not leave computers or other city devices unattended and screen unlocked with confidential files open.
 - c. Lock up and store computer media such as USB sticks and portable hard drives with confidential data.
 - d. Lock up any confidential printed records, photos, etc. whenever leaving a workspace or other place where they may be unsecured for any period of time or where they may be viewed by visitors to the work space who are not authorized to access those documents.
 - e. Ensure that screens are positioned in a manner so persons not authorized to have access to confidential information cannot view it when it is on the screen.
 - f. Ensure that electronic communications containing confidential information cannot be accessed by unauthorized persons. This may require using encryption for such communications. It may require that unauthorized colleagues do not have access to emails or folders.
 - g. Ensure that oral communications, especially those using electronic devices (such as cell phone, telephone, Zoom, MS Teams, or other electronic communications) that use or refer to such confidential information cannot be overheard by anyone who is not authorized to have the information.

§7 – Security.

A. Security Risk. As described in the Community Commitment at the beginning of this policy, the security of the computing environment is frequently challenged and consequences of failures in the security of the computing environment can be devastating. Security challenges continually increase in frequency, sophistication, technical acumen, guile, subtlety, and, sometimes, sheer computing forcefulness. Best defensive practices are continually evolving but wariness and persistent vigilance are key to defensive success.

B. Security Responsibility. It is the responsibility of every user of the computing environment to use and operate electronic devices in ways to minimize security risks to the computing environment and city devices including, for example and not for limitation, unauthorized access to, corruption of, damage to, or loss of, any part of the computing environment, any city device, the personal devices of other users, city content or other content on the computing environment, or the reliability of any part of the computing environment or city devices.

C. Passwords.

- 1. For applications that do not use the network login as credentials, the user must have a unique, strong password for each secure part of the computing environment that is accessed. Having the

same password for all systems accessed, is a security risk. To manage passwords, use of “password managers” is encouraged.

2. Passwords may not be shared among users and must not be written down and left accessible to others.

3. The IT director, with the consent of the city manager, will distribute and implement a password policy with requirements for password length, expiration period, and other requirements, that will change with recommended best practices.

4. Current password requirements, as of the date of this policy, are:

- a. Passwords will expire every 90 days and require changing.
- b. Passwords must be a minimum of 12 characters in length.
- c. Passwords must include 3 of the following 4 items:
 - (i) Upper case letter.
 - (ii) Lower case letter.
 - (iii) Number.
 - (iv) Special Character (e.g., #, ?, \$, *, @, etc.).

D. Multi-factor Authentication. While not required by all systems, multi-factor or dual-factor authentication is an industry recommended standard requirement. It is an extra layer of security that requires, not only a username and password, but also something that the user has on them, usually a temporary code pushed by text or email, to complete login. If the city device or computing environment system has a multi-factor or dual-factor authentication option, users will be notified it is available, how to use it, and required to turn it on and use it.

E. Security Training.

1. Security training required for all city personnel who are users and may also be required for other users.

2. The IT director will initiate a security training program and track completion. Details of the current *IT Security Training Plan* are located on the city’s Intranet, under “*Online Support*.”

3. Security training is included in an IT orientation session provided to new employees and is available for current employees.

4. The city will occasionally use Phishing or other tests to assess users’ safe email and other practices. Those who fail will be required to take remedial training. Test failures and incomplete training are automatically reported to employees’ supervisors.

F. Responsibility to Recognize and Report.

1. All users must immediately report any (i) unauthorized access or access attempts, (ii) virus infection, (iii) spyware infection, or (iv) any other unauthorized resource use, to the IT help desk, an IT department employee, or the user’s supervisor (if the user is a city contractor, to the city personnel with whom the user is working).

2. Users must report suspicious emails by using the city-provided phishing reporting tools and/or contact the IT help desk for further investigation.

3. City employees must question and/or immediately report individuals who are in areas that could be used to infiltrate the computing environment or in areas where confidential information may be located. For example, a city employee observing an unrecognized individual sitting in the council chambers with a laptop attempting to plug into a network floor-jack should immediately report that observation to the IT Department or a department director. Similarly, if an employee observes an unknown person entering an office area in the absence of its normal city personnel, that observation should be immediately reported to a department head or supervisor.

G. Account Lockout Due to Password Expiration or Other Reason.

1. Users (and, for city personnel, their supervisors) will receive an email daily, beginning 15 days before their password notifying them of the need to change their password. Users must login and

change their password before it expires. Information Technology will periodically review a report of users who have not changed their password, and will disable the user accounts, requiring a user to contact the help desk to have their account enabled.

2. Account lockout may also occur if a user fails to complete training, fails to incorporate multi-factor authentication when directed to do so, or fails to comply with any other provision of this policy.

§8 – Appropriate Use.

A. General Expectations and Requirements. Access to and use of the computing environment and city devices must comply with this policy. The computing environment and city devices are provided to conduct city business. Access to or use of the computing environment and city devices for other than city business must be limited as provided in this policy. Users must conserve and protect the computing environment and city devices for the benefit of public interest.

B. Software and Applications.

1. Only software and applications approved by the IT department may be installed in the computing environment or on city devices. All users must consult IT department staff before installing software or applications on the computing environment or a city device. Doing so enables IT department staff to:

- a. Ascertain that applicable license fees and license requirements are met.
- b. Ensure compatibility with the computing environment, city device, other software and applications in use, cellular or other service providers, and anticipated changes in any of them.
- c. Ascertain that the appropriate versions are used.
- d. Assist with installation and provide instruction or guidance on appropriate settings and permissions.
- e. Provide guidance and, when needed, warnings about uses, limitations, etc. This may include passing on helpful information from other persons using the software or application.
- f. When appropriate, suggest alternatives.
- g. Ensure any related pricing is appropriate.
- h. Ensure license agreements have been reviewed and approved as required by city policy.
- i. When appropriate discourage or prohibit installation.

2. Only properly licensed software may be installed within the City's Computing Environment. Use of unauthorized, unlicensed, or improperly licensed software is not acceptable. Unlicensed or improperly licensed software is subject to removal, with or without notice to the user.

3. Only applications from an industry standard store, such as the Apple Store or Google Play Store, may be installed on a device. Permissions should be granted only for those functions and features required for the application to run correctly.

4. Users must not duplicate, copy, reproduce or transfer any software purchased by and/or licensed to the city, or any related documentation without prior written approval from the IT director.

5. City personnel must not allow any other persons (including, for example and not for limitation, clients, contractors, customers, citizens, residents, other governmental officials, etc.) access to, use of, or copies of any city-purchased software or software licensed to the city without prior written approval from the IT director. (In certain instances, some Cloud software providers allow employees to run copies of their software in the home and on personal devices if licensed to the employee in the workplace. Seek guidance and approval for this type of arrangement from IT and your supervisor.)

C. Copyrighted Material - Intellectual Property Rights.

1. The computing environment and city devices must not be used to obtain, store, create, copy, transfer, install, or use unpurchased, unlicensed, unleased, or otherwise illegal copies of copyrighted materials, including for example and not for limitation, music, videos, photos, books, magazines, newspapers, podcasts, software, applications, data, information, or other materials or content. Illegal copies of materials or content are subject to immediate deletion upon discovery.

2. Software and work product (e.g., documents, databases, spreadsheets, programs, scripts, etc.) developed by employees or contractors working on behalf of the City, for City projects, shall be the property of the City. Such software and/or work products are for the exclusive use of the City, its

officers, agents, and employees. Such software and/or work products may not be sold, transferred, or given to any person without the prior written approval of the City Manager or designee, unless authorized as a normal part of the employee's day-to-day duties.

D. Use of City Email. City email accounts are provided to most city personnel for city business. The same standards of decorum, respect, and professionalism applicable to in-person interactions apply to the use of email. For examples, the following email activities are prohibited:

1. Using a city email address for personal emails, such as banking statements, credit card, and bill payments is not allowed.
2. Obtaining, accessing, or distributing another user's email account unless authorized by the account owner.
3. Transmitting city records, data, information, or other materials or content, within or outside the city, without authorization.
4. Transmitting "unencrypted" or un-confidential emails of data that is required to be encrypted. See §6.B.1. Consult your supervisor if you have questions on email encryption requirements.
5. Using a city email address for a personal business activity, other employment, hobbies, job searches, house hunting, vacation searches or arrangements, searching for or purchasing concert or event tickets, or personal shopping.

E. Personal Email Access and Use.

1. Use of a device directly connected to the city's network to access personal email accounts is prohibited. City email has many protections, such as email scanning services and filters to help protect against malware and undesirable introduction of destructive content into the City's network. Accessing personal email on a network-connected City computer, bypasses these filters and places the City at risk.
 - a. Using a city desktop computer directly connected to the city network (e.g., at a workstation in city hall, one of the utility plants, the public works building, the police building, a fire station, or the court building) to access personal email is prohibited.
 - b. Using a city laptop connected to any city wireless network to access personal email is prohibited.
2. Users may use personal devices, such as personal tablets or personal cell phones, connected to the city's "guest" or "internet only" wireless networks to access personal email.
3. Users may use a city cell phone or personal cell phone to access personal email.
4. **Using a personal email account or a personal cell number to text message to conduct city business** (e.g., communicating on behalf of the city or performing tasks as city personnel) **is prohibited**. Exceptions to this prohibition may be authorized by a city department head after consulting with the IT director.

F. Personal Use of City Devices and Computing Environment. Personal use of city devices and the computing environment must not be excessive or otherwise unreasonable. Any personal use of city devices and the computing environment is subject to the same privacy limits (see §5) as any other use of them.

1. The city allows occasional personal use on breaks and during non-working hours with supervisor approval. Personal use must not interfere with the performance of job duties.
2. Bandwidth to the Internet is a shared, finite resource. Thus, users must not use it in ways that adversely affect other city personnel or the performance of city business. If uncertain about a use activity, city personnel should check with supervisors or IT department staff.

G. Internet Use. The city recognizes the Internet can be a valuable, needed resource to conduct city business. It therefore provides that access to city personnel via city devices and the city computing environment. However, use of the Internet via city devices or the computing environment can increase security risks. It also occupies bandwidth. Therefore, the following apply to its use:

1. On-line services and the Internet are to be used for city business purposes. Personal access and use should be limited as expressed in the preceding subsection 8.F. Department directors and supervisors may, with approval of the IT Director and City Manager, establish written procedures and guidelines for personal access of the Internet.
2. Except when directly related to city business, City personnel must not use a city e-mail address to register at an Internet site (e.g., banking, shopping, and personal bill payment sites). Also see subsection 8.D above.
3. City personnel must not use a City e-mail address to register for the receipt of non-business e-mail lists (e.g., joke of the day, horoscope of the day, etc.). Also see subsection 8.D above.
4. Internet bandwidth must not be used for, and may be throttled back or blocked for, bandwidth-intensive activities not reasonably needed to conduct city business (e.g., music streaming, video streaming, streaming of a sporting event or celebration, news streaming, etc.).
5. The city may monitor the Internet activities of all users and may review the contents of stored Internet access logs. See §5.
6. The City may utilize Internet content filtering or website blocking.

H. File Storage and Encryption. Unless otherwise directed by a department director, the following will apply to file storage:

1. Users must store all important, confidential, or proprietary information on the LAN.
2. Files are to be stored unencrypted on the LAN so city personnel can access the information should the need arise in the absence of the storing user.
3. Storing information on a desktop, laptop or tablet device is discouraged as it can result in (i) content loss in the event of a computer drive failure, (ii) less security, and (iii) an inability to retrieve previous versions of files when needed due to file deletion or corruption or desired for another reason.
4. Department directors may direct users to store some information in encrypted formats or using other designated security when needed to secure confidential content (see, e.g., §6).
5. User are responsible for understanding the filing system and storing content in the appropriate network location to ensure proper security and access permissions as well as organization.

I. Cloud Computing. Cloud computing offers advantages including lower costs, high performance, and quick delivery of services. However, without adequate controls, it can expose the city to increased risks such as data loss or theft, and unauthorized access to the computing environment. These provisions are intended to establish process so users can use Cloud computing services without jeopardizing city data, city devices, or the computing environment.

1. The following applies to all users and all external Cloud computing services, e.g. Cloud-based email, document and file storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.:
 - a. Cloud computing services must not be used or accessed by any user on any city device or the computing environment,
 - b. No city data, information, software, files, or other content may be transmitted to any Cloud computing service,
 - c. No Cloud services accounts may be opened, or Cloud services contracts entered into, and
 - d. No Cloud services software, applications or files may be downloaded to any city device or the computing environment,

without prior approval of affected department director and the IT director. Either may also consult the city manager before giving approval. Any user who is unsure whether a service is Cloud-based or not, is expected to contact the IT department.

2. The IT director must determine that security, privacy, and all other aspects of the propose Cloud computing service comply with (i) this policy, (ii) applicable legal requirements, including any confidentiality requirements, (iii) requirements related to particular contracts, such as grant agreements, (iv) records retention requirements and schedules, and (v) any other requirements.

Some Cloud computing services meet specified government protocols. Others might not.

3. Any contracts for Cloud computing services must be reviewed, approved and signed in the same manner as other city contracts.
4. Users of Cloud computing services must not share log-in credentials with others.
5. For business continuity purposes, the IT department will establish a registry of services and departments using Cloud computing service must provide an administrative login to the IT department for any Cloud computing services.
6. Use of Cloud computing services must comply with all laws and regulations governing the handling of personally identifiable information, City financial data or any other data owned or collected by the City of Wyoming.
7. The IT director will determine what files, information, data and content may or may not be stored in the Cloud.
8. Personal Cloud computing services accounts must not be used for the storage, manipulation or exchange of any city files, information, data or content.
9. Files, data, information, and content stored in the Cloud must be duplicates of files that exist on the LAN, not originals. If originals are in the Cloud, the city risks their loss due to mistaken deletion, Cloud failure or breach, Cloud backup failure, bankruptcy of a Cloud service provider, etc. Users may only use Cloud storage services pre-approved by the IT director. Currently, the City contracts with a Cloud-based office suite environment (Microsoft Office 365) that offers a Cloud storage solution. This cloud-based solution is pre-approved for use and offers more security than others, such as City data is stored in the "Government Cloud," which is a segmented Government Cloud community that enables organizations to meet federal compliance and security standards.
10. There are methods for using Cloud products that allow ease of synchronization between city devices and the Cloud. Users must contact the IT department for direction on proper use of the Cloud for protection against data loss.

J. Prohibited Use.

1. In addition to those already stated in this policy, the following are prohibited uses of city devices and the computing environment (unless the specific use is expressly authorized by law or the appropriate city management staff) except when necessary for law enforcement or other investigative purposes, reasonably needed to perform some other city business, or when approved by the city manager.
 - a. Sending, receiving, transmitting, storing, possessing, creating, editing, or modifying any information, materials, or content contrary to any laws, rules, regulations, orders, or legal rights. Any user receiving any such information, materials, or content, should immediately report it to a supervisor, department director, the IT director, or city manager.
 - b. Sending, receiving, transmitting, storing, possessing, creating, editing, or modifying any information, materials, or content that is or could be understood by others to be in violation of the civil rights policy or any other city policy. Any user receiving any such information, materials, or content, should immediately report it to a supervisor, department director, the IT director, or city manager.
 - c. Sending, receiving, transmitting, storing, possessing, creating, editing, or modifying any information, materials, or content that is defamatory. Any user receiving any such information, materials, or content, should immediately report it to a supervisor, department director, the IT director, or city manager.
 - d. Sending, receiving, transmitting, storing, possessing, creating, editing, or modifying any information, materials, or content that is not authorized to access or to communicate or transmit.
 - e. Sending, receiving, transmitting, storing, possessing, creating, editing, or modifying any information, materials, or content that is confidential to any persons or in any manner except as authorized.
 - f. Sending, receiving, transmitting, storing, possessing, creating, editing, or modifying any information, materials, or content that, if publicly disclosed would invade the privacy, cause

embarrassment to, lead to misapprehensions about, or cause emotional harm to another individual. Any user receiving any such information, materials, or content, should immediately report it to a supervisor, department director, the IT director, or city manager.

g. Sending, receiving, transmitting, storing, possessing, creating, editing, destroying, or modifying any information, materials, or content in violation of Michigan's Open Meetings Act, Michigan's Freedom of Information Act, or records management, retention and disposal requirements, policies and schedules. Any user receiving any such information, materials, or content, should immediately report it to a department director, the IT director, or city manager.

2. Subsection 8.J.1.f does not impair the First Amendment rights of any city personnel to disclose matters of public concern to the extent permitted by law.

K. Use Cautions. Some uses of city devices or the computing environment may be unwise even if they are not prohibited. Records on electronic devices are often nearly permanent. (Even if later removed or deleted, others may have made copies, taken screen shots, etc.). The following are use cautions all users are expected to heed.

1. A good rule of thumb for users is, "If publication or broadcasting on national media would embarrass you or those you care about, don't put it in a text, email, voice message, image, etc. Don't create it. Don't transmit it. Don't say it. Don't repeat it. Don't forward it. Don't have anything to do with it."

2. A second good rule of thumb is, "It isn't humorous if another group of persons would view it as offensive, off-color, derogatory, etc.," and it doesn't belong on a city device or the computing environment.

3. If you are angry when first composing a written message, wait until at least the next day before sending it. Don't leave a voice message when you are angry.

4. For any use of a city device or the computing environment, ask yourself whether your colleagues, supervisor and department head would approve.

5. Avoid the use of personal devices when communicating as part of any city business. Use of a personal device may subject that device to a forensic examination by outside parties.

§9 – Personal Devices.

A. City Rights. The city reserves the right to determine if and in what manner personal devices will be allowed to interact with the computing environment.

1. The city is not required to allow interaction with any personal device or with any type, make, or model of personal device.

2. When interactions are allowed between a personal device and the computing environment, the city is not required to support proper functioning of that device.

3. The city may at any time, for any reason, suspend or discontinue allowing any particular personal device, any user of a personal device, or any program or application on a personal device from interacting with the computing environment.

4. The city may take steps the city, in its sole discretion, deems prudent to protect city data on a personal device, up to and including remotely triggering actions that prevent use of the personal device or that permanently erase all information on the personal device. The city may also require installation of certain software a personal device before its access to the computing environment is permitted.

B. Permission Required. Interaction of personal devices with the computing environment will require the IT director's written approval based upon a written request from the director of the department to which the user is assigned (*Personal Owned Mobile Device Request form* located on the city Intranet under forms). If approved, IT department staff attempt to connect the personal device to the computing environment and will verify the device meets required security standards. If not approved, the request will be returned with a written explanation.

§10 – Physical Security.

Physical security is key to protecting electronic devices, the computing environment, and information, data and other content from loss and damage. Many city work areas are accessible to persons who are not authorized to access certain devices, files, data, information or other content, so physical security is critical. Some the following measures are legally required for some data and information, for some uses and applications, for some users, and in some locations.

A. Auto-lock. City computers are configured to auto-lock after 30 minutes of inactivity. Other city devices are also configured to auto-lock.

B. User Lock and Logout.

1. Users leaving a desk or work area must manually lock screen before leaving (press and hold the “Windows Key” and then the “L” key to lock your computer).
2. Users must logoff at the end of the shift, except if otherwise permitted by the IT director.

C. Securing Devices and Information. Portable electronic devices (e.g., laptops, tablets, cell phones, etc.) must be secured in a locked file cabinet, desk drawer, vehicle (out of sight in the vehicle), or other locked location when unattended (even for a few minutes). Physical files, media, photos, printed copies of computerized information, and other records containing any confidential information (see §5) must similarly be locked when unattended.

D. Prohibited Device Connections. Users must not attach any form of network equipment, including, but not limited to switches, routers, hotspots, or any other device intended to be an intermediary data transport, to any city device or to the computing environment.

E. Device Loss, Theft or Tampering. Users must immediately report to the IT director the loss or theft of any city device or any personal device used to access or connect to the computing environment. Users must also immediately report to the IT director any incident where they suspect any person other than themselves or a member of the IT department staff may have or attempted to view, use, or gain access to any city device, the computing environment, or any personal device used to access or connect to the computing environment.

F. Equipment Relocation. Only IT department staff or city personnel directed by IT department staff may move any city devices other than laptop computers, tablets, cell phones and similar portable city devices. IT department staff may suggest alternatives, such as providing additional equipment instead of breaking down an existing workstation environment, for example, for “work from home.” The IT department also maintains locational inventories city devices that for, insurance and other purposes, need to be accurate.

§11 – Remote Access.

A. Allowed Use. This is to address remote use by users wishing to access the computing environment using either city devices from a location outside of city buildings and facilities or personal devices.

1. Remote access may be allowed pursuant to the Information Technology Procedures for Remote Access. If the remote access is the result of a “work from home” request, the city personnel must fill out the request form required under City *Telework Policy*, located on the Intranet under *Policies* (<https://info.wyomingmi.gov/hr/Telework%20Policy.pdf>), and get approval as listed on the policy. Once the *Telework Policy* is reviewed and approved, it is expected that the user working remotely review and abide by the *Secure Telework Guidelines* on the City Intranet, located under the *On-line Support* section.

2. Remote access required by vendors, consultants, and other non-City entities require the execution of a “*Acknowledgement of and Agreement to comply with City of Wyoming Policies*” agreement. Remote access is defined as “connecting to the City’s computing environment from any point external to that environment.”

B. Authorized Users and Devices. Secure remote access is strictly for city personnel and individual personnel of approved city contractors. Users with remote access must not allow any other individual to use their connection, nor share their password or other information needed to gain access. This policy applies to all electronic devices used to access the computing environment.

C. Approved Access Methods. IT department staff must evaluate and approve all remote connection methods compliance and security. The IT department staff will select the most appropriate and secure access option for the specific request.

D. VPN Approval. An user requesting Virtual Private Network (VPN) access, must submit an online request on the Intranet, under *Forms: Virtual Private Network (VPN)*. This automated process will route the request for various approvals, such as the department supervisor and IT department. Once approved, a VPN access request will be automatically sent to the help desk and the user will be contacted by IT department staff to schedule implementation. All VPN access forms will be periodically re-evaluated (currently annually) and reapproved by the user's department director IT department.

§12 – Electronic Device and Software Acquisition.

All city acquisition of electronic devices, software, applications, information technology services, and related items, products or services requires the prior written approval of the IT director and must be completed in accordance with city purchasing policies. IT department staff Information will meet annually with departments to budget for and plan annual replacements for updating computer equipment and software to prevent obsolescence. Purchases requested outside of the annual planned replacements are to be reviewed by IT department staff and the director of the requesting department.

§13 – Disposal of City Devices.

A. General Disposal by IT Department. Sale and disposition of city devices will occur in accordance with the City Charter, City Code, city purchasing policies and the city theft policy. IT department staff will manage the disposal of city devices. To be clear, no city personnel or any other user is authorized to dispose of any city device except IT department staff.

B. Cell Phones. Disposal of cell phones is outlined in the finance department document entitled, "*Cell Phone Replacements/Plan Changes*," or if not replacing per that document, cell phones are to be delivered to the IT department for disposal.

§14 – Information, Data and Content Disposal.

All city records (*i.e.*, all hand or machine produced, paper or electronic, photographic, video, audio, pictorial or other records in any format or form) are subject to city records retention and disposal schedules and requirements regarding their safekeeping and public access from the time of their creation through the time of their destruction or other disposal. Consequently, the IT department and city clerk will together review and handle the disposal or destruction of any city records, data, information, and any other content on any city device or the computing environment. No other city personnel and no other user is authorized to do so unless specifically designated in writing (*e.g.*, a confirming e-mail) by the IT director and/or city clerk.

§15 – City Messaging.

To ensure city messaging is accurate, clear, complete, timely, consistent, helpful, appropriately directed, properly distributed, and appropriately precise, no city personnel except those designated by the city council, the mayor, or the city manager are authorized to make any statements, take any positions, or release or disclose any information for or on behalf of the city. It is also imperative that all city communications be retained, disclosed, and disposed of in accordance with applicable law and legal obligations, including for example and without limitation, the city's records retention and disposal policy.

A. Prohibited Messaging.

1. No city personnel, except those designated by the city council, the mayor, or the city manager, shall make any statement, take any position, or disclose any information on for or on behalf of the city via any electronic device.
2. Regardless of the electronic device used to do so, no city personnel, except those designated by the city council, the mayor, or the city manager, shall make any statement, take any position, or disclose any information, image or recording for or on behalf of the city on via any social media (*e.g.*, Twitter, Facebook, etc.).
3. Regardless of the electronic device used to do so, no city personnel, except those designated by

the city council, the mayor, or the city manager, shall make any statement, take any position, or disclose any information, image, or recording on any social media in any manner that others could perceive is made, taken or disclosed in the poster's capacity as city personnel. This provision does not apply to city council members.

B. Prohibited Use of Personal Device. No city personnel shall make any statement, take any position, or disclose any information for or on behalf of the city on via any personal device.

§16 – Social Media.

The city maintains its website and social media sites, primarily to communicate with the public about matters of interest related to the city. Use of these sites will be actively monitored by city personnel designated by the city manager. The following policy will be followed and will be posted on city sites:

City of Wyoming social media pages are regulated and maintained by designated city personnel. We welcome your comments. We actively monitor our pages and try to respond to each inquiry. While we encourage discussion and debate, we request commenters stay respectful and on topic. A comment may be deleted if it violates the following comment policy.

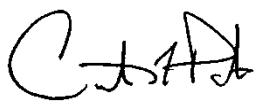
- Comments not related to the business or work of this department/office or to the particular social media article being commented upon may be deleted.
- Multiple or repetitive posts that are copied and pasted may be deleted.
- Obscene, violent, profane, sexual, or harassing language is not allowed. Links to sites containing obscene, violent, profane, sexual, or harassing content are not allowed.
- Statements that are defamatory, libelous, knowingly false, or stated reckless disregard for the truth are not allowed.
- Copyrighted material posted without permission or content that violates the legal ownership interests of another party is not allowed.
- Commercial advertisement or solicitation is not allowed.
- Comments that suggest or encourage illegal activity are not allowed.
- Information that may compromise the safety or security of the public or public systems is not allowed.
- Personal information such as identification numbers, phone numbers, or email addresses should not be posted and may be removed.
- We strictly prohibit discriminatory messages. We will delete hateful speech of any kind toward any group, including age, gender, race, religion, nationality, sexual orientation, or disability.
- Do not report emergencies or ask for assistance on this page. Call 911.

CERTIFICATION

By my signature below, this plan is an Administrative Policy of the City of Wyoming.

By signing below, I certify that to the best of my knowledge and belief:

1. This plan received any required reviews under applicable collective bargaining agreements.
2. This plan was either prepared by or reviewed and approved by the City's Information Technology Director.
3. This plan complies with applicable federal and state laws, rules, regulations, permits, and licenses, and with applicable contract requirements.



Curtis L. Holt, City Manager

Date signed: July 13, 2021

City Employee Receipt of Information Technology Policy

I have received and read the City of Wyoming Information Technology Policy ("IT Policy").

I acknowledge I must comply with the IT Policy and consequences for noncompliance are the same as for noncompliance with other policies, which may include disciplinary action up to and including termination of employment.

I understand that if I have any questions about the IT Policy, its implementation, or what it requires of me, I should ask my supervisor.

I understand the City of Wyoming can modify the IT Policy at any time.

I understand that, during any work for the City of Wyoming, I am required to act in a professional manner, and appropriately use all city equipment and its computing environment.

Employee signature: _____ Date signed: _____, 2021

Employee's name printed: _____

Non-Employee User Receipt and Acknowledgement of Information Technology Policy

I have received and read the City of Wyoming Information Technology Policy ("IT Policy").

I acknowledge I must comply with the IT Policy.

I understand and acknowledge I must comply with all provisions applicable to "users" as defined in the IT Policy.

I acknowledge that consequences for noncompliance with the IT policy may include any one or more of the following: (i) immediate termination of all access to City of Wyoming information technology systems and devices, (ii) termination of any contractual or other relationship with the City of Wyoming, (iii) ineligibility to bid on, be a party to, or provide any goods or services under future contracts with the City of Wyoming, (iv) other consequences as may be provided in any contract that I or my employer may have with the City of Wyoming, and (v) other consequences as may be provided under applicable laws, rules, regulations, ordinances, permits, licenses, and contract provisions.

I understand that if I have any questions about the IT Policy, its implementation, or what it requires of me, I should contact the City's IT Director.

I understand the City of Wyoming can modify the IT Policy at any time.

I understand that, during any work for the City of Wyoming, I am required to act in a professional manner, and appropriately use all "city devices" and its "computing environment," as those terms are defined in the IT Policy.

User's signature: _____ Date signed: _____, 2021

User's name printed: _____

Name and address of User's business or employer:

